

Project Brief

Jasmin Kaur Rai, jkr1g17

October 21, 2019

1 Agreed Project Title

An investigation into bot detection using network traffic analysis.

2 Supervisor

Nawfal Fadhel

3 Agreed Project Description

3.1 Problem

Many devices nowadays are hijacked into botnets with no sign of access, this is contributing to larger issues such as DDoS attacks. Many corporate networks can have their resources taken hostage or slowed down by these bots. With regards to an IoT society that we see coming into fruition today, we want to direct the problem towards IoT devices and their susceptibility to vulnerabilities that might expose themselves to network analysis. Thus the problem we will be addressing throughout the project is the detection and analysis of bots across a network consisting of IoT devices, using network traffic analysis tools.

3.2 Goals

The goal of this investigation is to be able to detect bots on a network using network traffic analysis, by using patterns and anomalies to uncover when a bot exist. One of the other goals of the investigation is to discover what vulnerabilities lie in IoT devices specifically, By the end we will propose a analysis solution for detecting bot activity on a network running IoT devices.

3.3 Scope

In this investigation we will cover a scope specific to IoT devices as well as a client-server modelled network. We will specifically focus on the analysis of the impact of bot running on the network as well as on IoT.